NORTH DAKOTA

HOMELAND SECURITY

ANIT-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Fargo phone troubles fixed. Telephone service was restored to city departments in Fargo, North Dakota, that were experiencing outages April 17. Throughout the day April 16 and the morning of April 17, the following departments did not have phone service: Public works, streets, mains & hydrants, forestry, solid waste, environmental health, and the sump pump program. The outage included the main numbers as well as individual extensions throughout each department. Source: http://www.valleynewslive.com/story/17506412/fargo-phone-troubles

Regional

More flood storage has limited benefit to Missouri River. More flood storage space in the Missouri River's reservoirs would have reduced, but not prevented, the devastating floods of 2011, the U.S. Army Corps of Engineers said in a report released April 13. The Corps said there still would have been widespread flooding damage in 2011 because of the massive volume of water that moved through the river. It also noted that any increase in the amount of flood storage space in the reservoirs would reduce the economic benefits the river offers through barge traffic, recreation, and hydropower. Reducing flood risk along the Missouri River over the long run might require changing the way communities and states think about development in the flood plain and widening the levee system to allow for more room in the channel, the commander of the Corps' Northwestern Division said. In 2011, flooding caused at least $630 million of damage to flood control structures along the 2,341-mile-long river. Hundreds of thousands of acres of farmland also were damaged along the river, which flows from Montana through North Dakota, South Dakota, Nebraska, Kansas, Iowa, and Missouri. The latest report is part of the analysis being done to determine whether the Corps needs to increase the 16.3 million acre-feet of space that is normally cleared out each spring for flood-control purposes. Source: http://www.kansascity.com/2012/04/13/3555630/more-flood-storage-in-reservoirs.html

(Minnesota) **Drug thefts surge at Minnesota hospitals, medical outlets.** Reports of theft or loss of controlled substances at hospitals and other health care facilities in Minnesota jumped 325 percent from 2006 to 2010, according to a report released April 18 by the Minnesota Department of Health. The data on the increase in drug diversions in Minnesota comes from a health department analysis of reports to the U.S. Drug Enforcement Agency (DEA). In 2005, there were 16 reports to the DEA from hospitals and other health care facilities in Minnesota of theft or loss of controlled substances. By 2010, the annual tally of such reports grew to 52. The numbers released provide context for a series of high-profile incidents during the past 16 months in which health care workers were accused of taking painkillers from patients. In the wake of such incidents, the health department formed a coalition with hospitals, health care providers, and law enforcement to identify a set of best practices to improve security for controlled substances. Source: http://www.twincities.com/ci_20424274

(Minnesota) **Highway 14 deemed more deadly than once thought.** Fatal crash data and range of possible improvements were part of a Highway 14 safety audit released by the Minnesota Department of Transportation (MnDOT) April 17. The data found that: Highway 14 between North Mankato and New Ulm, Minnesota, is even more deadly than previously reported; construction of a four-lane expressway along the most dangerous stretch is less expensive than anticipated; and state transportation officials are likely to opt for quicker, less expensive fixes than an expressway. While Highway 14 has been expanded to four lanes most of the way from Rochester to Mankato, a 2010 Mankato Free Press examination of accident statistics found the two-lane segment from North Mankato to New Ulm had a fatal crash rate nearly double the rate for rural two-lane highways statewide. Several additional deaths have occurred since then, driving the crash rate on that segment of highway to three times higher than comparable two-lane highways around Minnesota. A broader look — adding crashes that included serious but not fatal injuries — showed a crash rate 50 percent higher than average. MnDOT's Mankato-based District 7 has made several low-cost improvements to try to reduce accidents, including rumble strips on the center line between the eastbound and westbound lanes. The 6.5-mile segment between North Mankato and Nicollet was identified as particularly perilous, along with the intersections between Highway 14 and other state highways at Nicollet and New Ulm. Source: http://mankatofreepress.com/local/x101451288/Highway-14-deemed-more-deadly-than-once-thought

(Minnesota) **Train spill in northwest Minnesota requires month-long cleanup.** Officials estimated April 16 it would take 2 more weeks to finish cleaning up 30,000 gallons of a petroleum-based chemical that spilled from a train car after a semi-trailer truck hit it March 31 in northwest Minnesota. The spill happened after the semi on U.S. Highway 59 struck an eastbound Canadian Pacific train at a crossing near Plummer, derailing at least one car. The truck's driver was killed. The impact punctured a 30,000-gallon rail tanker filled with aromatic concentrate, a flammable liquid. It pooled in a ditch where workers used booms to contain it. Officials closed 7 miles of Highway 59 and routed traffic around the spill site with detours now expected to remain in place throughout April. The sheriff said the closure was to divert motorists from "physical hazards" from heavy equipment brought in for the clean-up. The railroad, as part of a clean-up plan approved by the Minnesota Pollution Control Agency (MPCA), hired a company to monitor air at several locations in Plummer. So far, none of the tests have detected harmful levels of fumes, a MPCA emergency response program administrator said. Crews hired by the railroad began the week of April 9 to excavate soil contaminated by the liquid. It is being trucked to a lined pad about a quarter mile from the spill site, where equipment will be brought in to burn the soil. After the chemical in the soil is burned out, the remaining soil will be put in a landfill. Source: http://www.startribune.com/local/147678465.html

(Montana) **Coke dust release confirmed from Laurel's CHS refinery.** A dust cloud of coke dust released from the CHS Refinery in Laurel, Montana, April 13, prompted a Laurel elementary school to rush students indoors. Yellowstone County Disaster & Emergency Services director stated CHS officials confirmed the release of dust from the coker unit. The release occurred when one of the plant's coke drums was being cleaned with a high pressure water hose.

Officials with the state department of environmental quality and disaster & emergency services were alerted to the situation. The director said it does not appear the amount of coke released during the discharge was enough to be harmful. CHS officials sent cleanup crews to the scene of South Pond in Laurel, where the spokesman said one witness reported seeing a petroleum residue on the water. Source: http://www.ktvq.com/news/coke-dust-release-confirmed-from-laurel-s-chs-refinery/

(South Dakota; Nebraska; Iowa) **Corps reducing releases at Gavins Point Dam into Missouri River after heavy rain in Neb., Iowa.** The U.S. Army Corps of Engineers reduced releases from Gavins Point Dam near Yankton, South Dakota, from 28,000 cubic feet per second (cfs) to 22,000 cfs April 16 after a weekend of heavy rains. Similar reductions were under way at other upstream reservoirs. The chief of the Corps' Missouri River Basin Water Management Division said reductions were needed to prevent flooding along the Missouri River in eastern Nebraska and western Iowa. The river was expected to temporarily fall below the navigation target of 31,000 cfs in Sioux City. Source: http://www.therepublic.com/view/story/b8d6df31ce7a47d3baf174509bbb1a6a/NE--Severe-Weather-Missouri-River/

National

EPA will delay start of some U.S. fracking rules, API says. U.S. Environmental Protection Agency (EPA) rules for gas drilling will delay a requirement to capture air pollution at the well until 2015, the research director of the American Petroleum Institute said April 18. A delay in implementing some standards for new gas wells was a top demand of the group, which represents companies that drill for oil and gas. The EPA, which was scheduled to issue the rules April 18, rejected a bid by the group to exempt a number of wells from the requirements altogether, the research director said. The EPA proposed the rule in 2011 to focus on hydraulic fracturing in which millions of gallons of chemically treated water are forced underground to break up rock and free gas. The method has opened up vast new shale gas deposits and helped push natural gas prices to the lowest level in a decade. The original EPA draft would have put the rule into effect in about 60 days. The EPA rules will include incentives aimed at prodding drillers to use technology called green completions, which collects gas when a well is first tapped, according to the policy director for the climate and clean-air program at the Natural Resources Defense Council. Source: http://www.bloomberg.com/news/2012-04-18/epa-will-delay-start-of-u-s-fracking-rules-until-2015-api-says.html

International

Danger from Three Gorges Dam may force out 100,000. Authorities may force 100,000 people to move away from China's Three Gorges Dam in the next 3 to 5 years due to the risk of disastrous landslides and bank collapses around the reservoir of the world's biggest hydroelectric facility, state media said April 18. The ministry of land resources said the number of landslides and other disasters increased 70 percent since the water level in the $23 billion showcase project rose to its maximum in 2010. Some 1.4 million people already have been

resettled as a result of the huge project on the Yangtze River. Authorities may move people to minimize the risk of casualties from such threats, a ministry official told China National Radio. He said 5,386 danger sites were being monitored and that work was beginning on rockfalls and landslides at 335 locations around the lake. Fluctuations in water levels can trigger landslides and other problems, and the risks are accentuated by the density of the population, a recent report said. The government has acknowledged that filling the reservoir has increased the frequency of earthquakes, but the government denied it had anything to do with a powerful quake to the northwest in Sichuan May 12, 2008, that killed 87,000 people. Source: http://www.google.com/hostednews/ap/article/ALeqM5h_tTk1Mz94lKtgJIog3UT4xBK6aQ?docId=f550a6782c5d45da9c1398ff28da6548

U.S. issues emergency warning that radical Islamist sect may bomb hotels in Nigeria capital. The United States warned its citizens April 18 that a radical Islamist sect may attack hotels frequented by foreigners in Nigeria's capital. The is the second time the United States advised such an assault is possible in the widening sectarian fight in the West African nation. The warning offered no specifics about the threat posed by the sect known as Boko Haram, only saying the Nigerian government was aware and taking precautions to stop such an assault. The United Kingdom also issued an advisory to its citizens noting the U.S. message. Source: http://www.greenfieldreporter.com/view/story/ffd5e54b61fc4190b8cf172e276ded13/AF--Nigeria-Violence

Nigeria: Nema is prepared for Lake Nyos' collapse. The Nigerian National Emergency Management Agency (NEMA) said April 15 it is prepared for the imminent collapse of Lake Nyos near Nigeria's border with Cameroon, and the potential disaster it poses to Benue and other states in the country. NEMA's North-Central Zonal Coordinator said experts predicted the lake, a volcanic dam, would collapse by 2015. The collapse would cause the release of up to 50 million cubic meters of water into the Katsina-Ala River. "The water will flood Benue and Taraba states and release much carbon dioxide into the atmosphere," the coordinator said. "NEMA has installed warning signals in Kashimbila to warn people, about 10-kilometers away, of the possibility of a flood and advised that they be wary and ready for the lake's collapse if it eventually occurs earlier than the 2015 date." He advised the states to construct buffer dams to hold such excess water. A buffer dam was being constructed by the Nigerian federal government as a proactive measure to contain the effects of the lake's imminent collapse. Source: http://allafrica.com/stories/201204160846.html

Dak Lak: Broken dike not mended, causing heavy losses. According to local residents, a 32-meter section of the Suoi Cut dike in Dak Lieng Commonue, Lak District, Vietnam, broken in a flood October 2011 has never been repaired, causing water from the Krong Na River to flood the field of three communes in the region. The water level in the Krong Na River rose March 31 to April 2 through the broken dike, flooding nearly 1,300 hectares of rice. Thousands of families lost their crop. Total losses are estimated at over ($2.5 million). The authorities of Lak district said they requested around ($200,000) from Dak Lak province authorities to fix the broken dike, but the provincial government did not answer. The district needs capital to build a 1-kilometer dike along the Krong Na to prevent floods. Affected farmers have been supplied with rice and

seed for the summer-autumn crop. Source: http://english.vietnamnet.vn/en/society/21265/dak-lak--broken-dike-not-mended--causing-heavy-losses.html

Banking and Finance Industry

Web site stole job seekers' data in tax-fraud scheme. A Web site that promised to connect people with much-needed jobs during the recession was actually a means to steal applicants' personal information in a scheme to file fraudulent tax returns, prosecutors said April 17. The site, called jobcentral2, listed nonexistent jobs and used applicants' identities to file the bogus federal tax returns and collect tax refunds, the district attorney (DA) for the Manhattan borough of New York City said. A Russian citizen living in Brooklyn preyed upon unemployed people because they were unlikely to have income and unlikely to file a tax return, reducing the chances the fake returns would draw attention, the DA said. The man's site claimed its job placement services were "sponsored by the government and intended for people with low income," prosecutors said. He sent e-mails with links to his fake site through legitimate job search forums and college electronic mailing lists. He collected refunds in the names of 108 job seekers, an indictment said. The amount collected on each was about $3,500 to $6,500, which totaled more than $450,000. The man recruited 11 students from Kazakhstan, who let him use their bank accounts to cash the tax refunds, court documents said. He was charged with money laundering, identity theft, and other charges. Federal prosecutors in New Jersey, meanwhile, charged the same man April 17 with working with a ring that stole $1 million by hacking into retail brokerage accounts at Scottrade, E*Trade, Fidelity, Schwab, and other firms and executing sham trades. He was charged with conspiracy to commit wire fraud, unauthorized access to computers, and securities fraud. Source: http://www.nytimes.com/2012/04/18/nyregion/web-site-stole-job-seekers-data-in-tax-fraud-scheme.html

SEC charges optionsXpress and five individuals involved in abusive naked short selling scheme. The U.S. Securities and Exchange Commission (SEC) April 16 charged an online brokerage and clearing agency specializing in options and futures, as well as four officials at the firm and a customer involved in an abusive naked short selling scheme. The SEC alleged Chicago-based optionsXpress failed to satisfy its close-out obligations under Regulation SHO by repeatedly engaging in a series of sham "reset" transactions designed to give the illusion the firm had purchased securities of like kind and quantity. The firm and a customer engaged in these sham transactions in many securities, resulting in continuous failures to deliver. The former chief financial officer at optionsXpress was named in the SEC's administrative proceeding along with optionsXpress and the customer. Three other optionsXpress officials were named in a separate proceeding and have settled the charges against them. According to the SEC's order, the misconduct occurred from at least October 2008 to March 2010. The SEC alleges the sham transactions impacted the market for the issuers. For example, from January 1, 2010 to January 31, 2010, optionsXpress customers accounted for an average of 47.9 percent of the daily trading volume in one security. In 2009 alone, the optionsXpress customer accounts engaging in the activity purchased about $5.7 billion worth of securities and sold short about $4

billion of options. In 2009, the customer named in the administrative proceeding himself purchased at least $2.9 billion of securities and sold short at least $1.7 billion of options through his account at optionsXpress. Source: http://www.sec.gov/news/press/2012/2012-66.htm

Watchdog finds ongoing information security gaps at Federal Reserve banks. The Government Accountability Office (GAO) has identified ongoing information security gaps at Federal Reserve Banks, Infosecurity reported April 13. During previous audits, GAO identified information security gaps affecting internal control over financial reporting at the Federal Reserve Banks, which maintain and operate financial systems on behalf of the Bureau of the Public Debt. While GAO's audit for fiscal year 2011 did not identify any new security vulnerabilities, it found many existing gaps had not been fixed by the banks, although corrective actions are planned or in progress. "Additional actions are needed to fully address the open information systems control recommendations from our prior years' audits," GAO noted. "Until these information systems control deficiencies are fully addressed, there will be an increased risk that internal control deficiencies may exist and remain unidentified and an increased risk of unauthorized access, loss, or disclosure; modification of sensitive data and programs; and disruption of critical operations," the audit concluded. In response, the Director of the Reserve Bank Operations and Payment Systems said the banks "intend to implement corrective actions for one of the two remaining [gaps] by September 2012 as part of a transition to a new information security program, and complete actions to address the other [gap] in 2013." Source: http://www.infosecurity-magazine.com/view/25143/

GAO: SEC's financial information at risk. Government auditors have identified weaknesses in information security controls at the U.S. Securities and Exchange Commission (SEC) that jeopardize the confidentiality and integrity of the SEC's financial information, Gov Info Security reported April 13. Government Accountability Office (GAO) auditors uncovered four significant deficiencies in the GAO's review of 2010 and 2011 commission financial statements, including those involving information systems, according to a letter to the SEC chairwoman dated April 13. The GAO found the SEC had not consistently or fully implemented controls for identifying and authenticating users, authorizing access to resources, ensuring that sensitive data are encrypted or auditing actions taken on its systems. The SEC also had failed to install patch updates on its software, exposing it to known vulnerabilities, which could jeopardize data integrity and confidentiality, the auditors wrote. The SEC also did not configure servers supporting key financial applications to use encryption when transmitting data, resulting in increased risk that transmitted data can be intercepted, viewed, and modified. The GAO recommended the SEC create configuration baselines and related guidance to secure systems and monitor system configuration baseline implementation. Auditors also advised the agemcu to develop and implement a comprehensive vulnerability management strategy that includes routine scanning of systems and evaluation of such scanning. Source: http://www.govinfosecurity.com/secs-financial-information-at-risk-a-4679/op-1

Chemical and Hazardous Materials Sector

EPA issues air pollution rules for fracking wells. Federal regulators issued first-ever air pollution rules for "fracking" wells April 18, requiring that drillers burn or capture the gas and its smog-producing compounds released when the wells are first tapped. An Environmental Protection Agency official announced the rules, the first to cover some of the 13,000 wells drilled yearly nationwide that use hydraulic fracturing, or fracking, to collect natural gas and oil from deep shale layers. Going into effect in 60 days, they cover the period when a well is first drilled when natural gas is still venting but before it begins actual production. In a compromise with the industry, regulators said the drillers can flare, or burn off, the gas for now, a process that can last for weeks. However, starting in 2015 they would lose that option. Instead, they will be required to collect it — so-called green completion of new fracking wells. Half of all new wells already collect gases from the initial drilling of the well, but only Colorado and Wyoming explicitly require such green completions. Source: http://www.usatoday.com/money/industries/energy/environment/story/2012-04-18/fracking-pollution-rules-epa/54396226/1

NEI: American nuclear plants meet deadline to buy FLEX safety equipment. Every nuclear power plant in the United States has now purchased a long list of emergency equipment laid out in an industry-led effort to enhance preparedness following the 2011 crisis at the Fukushima Daiichi plant in Japan, Nuclear Street reported April 17. The Nuclear Energy Institute said all plant operators met the March 31 deadline to buy the items, some of which have already been received. The gear includes diesel-powered pumps, air-driven pumps for flood equipment, hoses, generators, battery chargers, electrical switchgear, cables, fire trucks, satellite communications, and items for emergency responders. The industry-favored FLEX strategy to enhance emergency preparedness seeks to place a wide range of equipment in diverse locations. It will be on hand for beyond-design-basis accidents, unforeseen events, and extreme natural disasters like those that blacked out the Fukushima plant. Source: http://nuclearstreet.com/nuclear_power_industry_news/b/nuclear_power_news/archive/2012/04/17/nei_3a00_-american-nuclear-plants-meet-deadline-to-buy-flex-safety-equipment-041702.aspx

Illicit strontium 90 deal busted in Armenia. Two Armenian citizens were detained following an attempted sale of radioactive strontium 90 in their home nation, Agence France-Presse (AFP) reported April 15. "Two residents of Yerevan [...] were arrested while trying to sell a radioactive substance, strontium 90," the Armenian National Security Service said in a statement. It did not provide specifics on how much material was involved or to whom the suspects allegedly intended to sell the strontium. In 2011, Armenia detained four nationals on suspicion of trying to sell strontium 90, AFP reported. Strontium 90 is considered a potential ingredient for producing a "dirty bomb," which would use conventional explosives to disperse radioactive material. It is among the highly radioactive materials that "require particular attention for safety and security reasons," according to the International Atomic Energy Agency. Source: http://www.nti.org/gsn/article/illicit-strontium-deal-busted-armeniatw/

EPA mulls new toxic report requirements. April 13, the U.S. Environmental Protection Agency (EPA) proposed a rule requiring electronic reporting of information to the agency under the Toxic Substances Control Act. Such a requirement would aid the agency in its effort to increase transparency and public access to chemical information, the EPA said in a news release. If the rule is finalized, the EPA said, it will only accept data, reports, and other information submitted through EPA's Central Data Exchange, a centralized portal that enables streamlined, electronic submission of data via the Internet. The agency said it would be soliciting comments on the proposed rule for 60 days. Source: http://www.upi.com/Science_News/2012/04/13/EPA-mulls-new-toxic-report-requirements/UPI-66641334358181/

(West Virginia; Ohio) **C8 linked to kidney, testicular cancer.** A three-person team of experts announced April 16 it has found a "probable link" between exposure to the chemical C8 and the development of kidney and testicular cancer in humans. Members of the C8 Science Panel made those conclusions in the second set of significant findings in their 6-year study of the DuPont Co. chemical plant near Parkersburg, West Virginia. Panel members cited previous studies of DuPont workers, as well as the results of their own still-to-be-published analysis of health data for thousands of Mid-Ohio Valley residents. The findings mean DuPont Co. will have to fund future medical tests for area residents, to help provide early detection of diseases linked to exposure to C8 from its Washington Works plant. Science panel members also said they found no probable link between C8 exposure and other cancers, saying they focused specifically on possible connections with disease of the pancreas, liver, prostrate and breast. Panel members also said they found no link between C8 and adult-onset diabetes. The work of this panel is part of the 2005 settlement of a lawsuit filed against DuPont by residents whose drinking water was contaminated. C8 is another name for perfluorooctanoate acid, or PFOA. Source: http://wvgazette.com/News/201204160035

Commercial Facilities

Trojan sneaks into hotel, slurps guests' credit card data. Cyber criminals are selling malware through underground forums that they claim offers the ability to steal credit card information from hotel point of sale (PoS) applications, The Register reported April 19. The ruse, detected by transaction security firm Trusteer, shows how criminals are using malware on enterprise machines to collect financial information in addition to targeting consumer PCs with banking trojans and other types of malware. The hospitality industry attack involves using a remote access trojan program to infect hotel front desk computers. The malware includes spyware components that steal credit card and other customer data by capturing screenshots from the PoS application. The malware is capable of stealing credit card numbers and expiration dates, but not CVV2 numbers in the sample Trusteer inspected. Trusteer said that at the time of publishing its blog April 18, the malware had not yet been detected by any anti-virus application. Source: http://www.theregister.co.uk/2012/04/19/hotel_trojan_scam/

Communications Sector

Nothing Significant to Report

Critical Manufacturing

Chemical plant shutdown could cut auto production. The potential shortage of a key component used to make fuel lines and brake lines could force automakers in the United States and around the world to close car and truck plants as they run short of parts, the Associated Press reported April 17. Auto industry executives scheduled an unprecedented meeting April 17 in Detroit to talk about the problem. Officials from as many as 10 automakers and dozens of parts supply companies were set to attend. A March 31 explosion at Evonik Industries in Germany killed two workers and damaged a factory that makes CDT. That chemical is a key component in a nylon resin called PA12, which is used to make a specialized plastic. The plastic is used in auto fuel lines and brake lines. PA12 has been in short supply for about 2 years, as demand from the solar industry increased. The Evonik incident will worsen the shortage, which could hit every major automaker. Source: http://www.mbtmag.com/news/2012/04/chemical-plant-shutdown-could-cut-auto-production

Defense/ Industry Base Sector

Scientists reprogram plant DNA to identify counterfeit military parts. A new technology that uses plant genes to track even the most miniscule computer parts is being considered to make sure sophisticated U.S. military equipment such as bomb guidance kits, airplane electronics, and radars are not being made with counterfeit components, according to an April 19 report by U.S. News & World Report. By reprogramming plants' genetic material, Stony Brook, New York-based Applied DNA Sciences can create a tiny marker that can be embedded on computer chips, mixed in with the ink used to print cash, or woven into clothing. The military can then use a device similar to a barcode scanner to instantly "read back" that DNA, verifying the parts are authentic. Experts have warned the electrical components inside some of the most sophisticated military computers are faulty and fraudulent, prompting Congress to pass a law in late 2011 requiring military contractors to guarantee the parts they use in military systems. The new tracking technology uses plant DNA because plants thrive in sunlight, whereas animals' DNA can break down from ultraviolet rays. In 2011, the U.S. military reported more than 1,300 counterfeit parts in their weapons — more than 4 times the 2009 number — to IHS iSuppli, a company that monitors the industry. Source: http://www.usnews.com/news/articles/2012/04/19/scientists-reprogram-plant-dna-to-identify-counterfeit-military-parts

Pentagon seeks to loosen some export restrictions. A U.S. Department of Defense report released April 18 recommended loosening U.S. export controls on "hundreds of thousands" of items used to build communications satellites and remote sensing equipment, while maintaining or tightening controls on exports to China, Iran, and other countries. The deputy assistant secretary of defense for space policy said the changes, if approved by Congress, would help make U.S. industry more competitive internationally at a time when defense budgets are declining. The Pentagon report comes as U.S. satellite makers and launchers, already dealing with cuts in funding for NASA programs, brace for cuts to national security satellite programs. To implement the changes, the report recommended Congress restore the President's

authority to determine export controls on the industry. Lawmakers revoked that power in 1999 after two U.S. companies were found to have provided unlicensed aid to China's space launch business. The report was welcomed by satellite industry executives, but it sparked concern among some lawmakers worried sensitive U.S. technologies would wind up in the wrong hands. The report lists the satellites and associated parts and components that can be removed from the U.S. Munitions Control list, overseen by the State Department and moved to the less cumbersome Commerce Control List with acceptable risk. The deputy assistant secretary of defense for space policy said the report recommended maintaining a ban on any U.S. satellites being launched by Chinese rockets, and put tighter controls on exports of satellites or components to China and other countries including Iran, North Korea, and Syria. Source: http://www.reuters.com/article/2012/04/18/satellites-exports-idUSL2E8FIF1R20120418

Nuke expert pool shrinking. Within the next half decade, the U.S. government expects to have lost to retirement all scientists who did hands-on work in the blueprinting and trial explosions of nuclear weapons, Defense News reported April 14. The small cadre of remaining personnel with that experience encompasses anyone who "had a key hand in the design of a warhead that's in the existing stockpile and who was responsible for that particular design when it was tested back in the early 1990s," the head of the U.S. National Nuclear Security Administration said in March. That loss of expertise is a significant issue for some observers who worry about the state of the nation's nuclear deterrent. Others say it should be expected given the nation's longstanding voluntary moratorium on nuclear-weapon trial explosions. It has been two decades since the United States last set off an underground blast. Some believe the United States should reserve the right to test its nuclear weapons not only to keep unique scientific and engineering skills alive, but also because the weapons may require it. However, a new report from the National Academy of Sciences says the country is able to maintain a safe and effective nuclear weapons stockpile without testing. Sustaining a high quality workforce remains one of the most important aspects of maintaining a safe, effective nuclear deterrent, the report says. Much of the scientific work being done on the weapons is called "surveillance," performing routine checkups on the weapons to make sure the components are still safe and functioning. Advocates of testing say surveillance is not reassurance enough that the warheads, which experience natural degradation over time, are still working. Source: http://www.defensenews.com/article/20120414/DEFREG02/304140002

Emergency Services

(Michigan) **Hackers attack Berrien County website.** Computer hackers gained access to the Berrien County, Michigan Web site April 15 and executed a plan the hackers called, "SSS = Shoot the Sheriff Sunday." Anonymous IRC, the name of the hacker group, placed material on the Berrien County Sheriff's Department Web site, including profanity and the group's views toward government agencies. After authorities learned of the cyber attack they quickly shut down the Web site. The Berrien County undersheriff said the county network was not compromised, and no personal information was obtained by the group beyond what was available on the county site and the sheriff's department site. Both Web sites are stored off site by an independent company and are separate from the county network. The county Web site

returned to service April 17, and the sheriff's department's site was back online April 18. The hackers gained access to password information for a select few county employees who had access to update and make changes to the Web site. Those passwords have been changed. Source: http://www.nilesstar.com/2012/04/19/hackers-attack-berrien-county-website/

(Oklahoma; Kansas; Iowa) **Experts: Don't rely just on tornado warning sirens.** When a tornado dropped quickly from the sky above Woodward, Oklahoma, April 15, the town's 20 outdoor tornado sirens were nonfunctional due to a lightning strike on the tower used to activate the warning system. The Woodward tornado proved fatal after it hit without warning. While it is unknown whether the disabled sirens contributed to the toll in Woodward, residents and officials in hard-hit areas of Kansas, Iowa, and elsewhere credited days of urgent warnings from forecasters for saving lives. Many residents have grown up counting on tornado sirens to warn them when a twister has been spotted on the ground, but emergency officials say that can be one of the least reliable methods, especially when a tornado hits at night. Emergency management officials urged residents to take advantage of weather radios, smartphones, and television warnings to keep them up to speed when weather turns dangerous. Sirens are not designed to wake residents who are sleeping or to penetrate the thick insulation in modern homes, the director of the Oklahoma Office of Emergency Management said. Source: http://www.cbsnews.com/8301-201_162-57414503/experts-dont-rely-just-on-tornado-warning-sirens/

Energy

Nothing Significant to Report

Food and Agriculture

Drought forecast for southwest, California 'not optimistic'. Most of the southwestern region of the United States as well as parts of California and the southeast can expect drought conditions to worsen through July, federal forecasters said April 19. "Overall, the current Drought Outlook is not optimistic," the National Weather Service said in summarizing its forecast. Besides affecting farmers and ranchers, drought means a greater risk of wildfires, especially in areas expecting a warmer than average spring. "May – July is expected to be warmer than normal" in the southwest and west, the service added in a more detailed report. "For most of the southwestern and western part of the country, drought is expected to persist in most locations and expand into the central Rockies," it added. "In addition, mountain snowpack, the source of a lot of the region's moisture, is starting off below normal, and as a result, summer streamflows are expected to be abnormally low," forecasters noted. Most of California and Nevada, as well as parts of Colorado, Oregon, Texas, Utah, and Washington state, are also forecast to see drought persisting or intensifying. On the East Coast, most of Georgia and South Carolina, as well as parts of Alabama, Delaware, and Maryland, are expected to see continued or worse drought conditions. Source: http://usnews.msnbc.msn.com/_news/2012/04/19/11288192-drought-forecast-for-southwest-california-not-optimistic?lite

Listeria concern prompts expanded deli sandwich recall. M.E. Thompson of Jacksonville, Florida, is expanding the recall of its Anytime Deli Turkey & Ham Footlong to include the Italian Footlong and Classic Cuban, sold under the brand names Anytime Deli, Sandwich Central, and Dandee, because the sandwiches may be contaminated with Listeria monocytogenes, Food Safety News reported April 19. The recall was the result of routine sampling by the Florida Department of Agriculture and Consumer Services, which revealed the finished products contained Listeria monocytogenes. According to the recall news release, no other finished products have been shown to contain Listeria since the original sampling. It said the latest recall is a precautionary measure. The initial recall was January 24. The sub sandwiches were distributed from January 2 through April 13 to convenience and grocery stores nationwide. Source: http://www.foodsafetynews.com/2012/04/listeria-concern-prompts-expanded-deli-sandwich-recall/

Sushi-linked Salmonella outbreak reaches 141 cases. A multi-state outbreak of Salmonella Bareilly infection has sickened at least 141 people, up from the 116 confirmed cases reported the week of April 9, while the related recall has expanded to include all frozen raw, yellowfin tuna product — called Nakaochi Scrape — distributed by Moon Marine USA Corp, Food Safety News reported April 18. Nakaochi Scrape is the backmeat of tuna that, when scraped off the bones, looks like ground tuna, and is used to make sushi and similar dishes. The Centers for Disease Control and Prevention (CDC) said Moon Marine's frozen raw Nakaochi Scrape tuna, imported from a single processing plant in India, is the likely cause of the outbreak. In an update April 17, the CDC said the illnesses extend across 20 States and the District of Columbia. New York has reported 28 cases; Maryland and Wisconsin 14; Illinois 13; Massachusetts 9; New Jersey and Virginia 8; Connecticut, Georgia, and Pennsylvania 6; Rhode Island 5; Missouri and Texas 4; Louisiana and South Carolina 3; Alabama, District of Columbia, Mississippi, and North Carolina 2; and Arkansas and Florida 1. April 13, the Cupertino, California-based Moon Marine agreed to recall 58,828 pounds of its frozen raw yellowfin tuna product, according to the Food and Drug Administration (FDA). In an update April 17, the FDA said Moon Marine is voluntarily recalling all frozen raw yellowfin tuna product from India, labeled as Nakaochi Scrape AA or AAA. The product is not offered for sale to individual consumers but went to outlets that used the tuna to make sushi and other dishes to be sold in restaurants and grocery stores. Source: http://www.foodsafetynews.com/2012/04/sushi-linked-salmonella-outbreak-reaches-141-cases/

Allergen alert: Milk in taco shells. Mission Foods recalled its Taco Dinner Kits distributed by Kroger, Winn-Dixie, Hannaford, and Food Lion because they may contain milk, an allergen not included on the label, Food Safety News reported April 16. The recalled products were distributed by Kroger in Indiana, Illinois, Missouri, Ohio, Michigan, Kentucky, West Virginia, Kansas, Nebraska, and Tennessee. Stores under the following names where Kroger operates are included in this recall: Kroger, Scott's, Payless, Owen's, Food-4-Less in Chicago, JayC, Dillons, Gerbes, and Bakers. The recalled products were sold in Food Lion stores in North Carolina, South Carolina, Tennessee, Virginia, Pennsylvania, West Virginia, Georgia, Florida, Maryland, Delaware, New Jersey, and Ohio. The recalled products were also sold in Winn-Dixie stores in

Florida, Louisiana, Georgia, Mississippi, and Alabama. Source: http://www.foodsafetynews.com/2012/04/allergen-alert-milk-in-taco-shells/

Moon Marine USA Corporation voluntarily recalls frozen raw yellowfin tuna product. Moon Marine USA Corporation of Cupertino, California, is voluntarily recalling 58,828 lbs of a frozen raw yellowfin tuna product, labeled as Nakaochi Scrape AA or AAA. Nakaochi Scrape is tuna backmeat, which is specifically scraped off from the bones, and looks like a ground product. The Nakaochi Scrape is associated with an outbreak of 116 cases of salmonella bareilly in multiple states: Alabama (2), Arkansas (1), Connecticut (5), District of Columbia (2), Florida (1), Georgia (5), Illinois (10), Louisiana (2), Maryland (11), Massachusetts (8), Mississippi (1), Missouri (2), New Jersey (7), New York (24), North Carolina (2), Pennsylvania (5), Rhode Island (5), South Carolina (3), Texas (3), Virginia (5), and Wisconsin (12). The product is not available for sale to individual consumers, but may have been used to make sushi, sashimi, ceviche and similar dishes available in restaurants and grocery stores. The product may have passed through several distributors before reaching the restaurant and grocery market, and may not be marked with lot information. Source: http://www.fda.gov/Safety/Recalls/ucm300412.htm

Dole Fresh Vegetables announces precautionary recall of limited number of salads. Dole Fresh Vegetables is voluntarily recalling 756 cases of Dole Seven Lettuces salad with use-by date of April 11, 2012, UPC code 71430 01057 and Product Codes 0577N089112A and 0577N089112B, due to a possible health risk from salmonella. Dole Fresh Vegetables is coordinating closely with regulatory officials, the U.S. Food and Drug Administration said April 14. No illnesses have been reported. The salads were distributed in 15 U.S. States: Alabama, Florida, Illinois, Indiana, Maryland, Massachusetts, Michigan, Mississippi, New York, North Carolina, Ohio, Pennsylvania, Tennessee, Virginia, and Wisconsin. This notification was issued due to an isolated instance in which a sample of Seven Lettuces salad yielded a positive result for salmonella in a random sample test collected and conducted by the State of New York. Source: http://www.fda.gov/Safety/Recalls/ucm300414.htm

Government Sector (including Schools and Universities)

(Washington, D.C.) **Laptops stolen from D.C. Auditor's Office.** Washington, D.C. police are investigating a break-in at the D.C. Auditor's Office during the weekend of April 14. Two laptop computers were among the several items stolen from the D.C. Auditor's Office, the council chairman's office confirmed April 18. Several interior doors were pried open to get in to the office, according to the police report. Source: http://www.msnbc.msn.com/id/47094177/ns/local_news-washington_dc/#.T5AM2Nk-N8F

New phishing scam targets military users receiving disability payments, DFAS warns. A new phishing campaign is targeting military service members, retirees, and civilian employees receiving disability compensation, the Defense Finance and Accounting Service (DFAS) warns. The e-mail scam dangles the prospect of additional disability compensation in an effort to get

recipients to give up their personal information, according to a post on DFAS' Web site, which urged anyone receiving such an e-mail not to respond to it. The e-mails, which appear to come from a DFAS employee, display a spoofed .mil e-mail address and say recipients of disability compensation from the Department of Veterans Affairs (VA) could also be eligible for money from the IRS, DFAS said. The phishing scam asks recipients to submit their VA award letters, income tax returns, 1099-R forms, and other documents to a supposed retired colonel in Florida. Phishing campaigns of this type — offering money for personal data — are fairly common around tax time, and phishing scams of all kinds are increasingly common in government circles, whether the goal is to compromise individuals' financial information or to attack enterprises. The U.S. Computer Emergency Readiness Team recently reported phishing was the most common type of attack against government networks, accounting for 51.2 percent of attacks. Source: http://gcn.com/articles/2012/04/16/dfas-warns-phishing-scam-targets-military.aspx

(Connecticut) **Security breach, 87,000 exposed.** A security breach into the hard-drive at Housatonic Community College in Bridgeport, Connecticut has affected nearly 87,000 people. College officials said they are taking action to make sure the students, faculty, and anyone on file stays safe. The breach does not just impact students who currently attend the college, it affects anyone who has a file on record in the hard drive. The date of birth and Social Security numbers of tens of thousands of people were exposed. Law enforcement is now involved. The school said even before the breach, the school dealt with on-line security on a daily basis. "For every individual whose record is there, we are providing two years of security insurance, security theft identification, if anything were to occur. Typically if there was to be a malicious attack, it's done within the two-year period," said the college president. Source: http://www.wtnh.com/dpp/news/fairfield_cty/security-breach-affects-thousands

Information Technology and Telecommunications

New Android malware spreads by text message. Criminals targeting smartphones crafted a clever text-message-based attack that removes the middleman and delivers its malicious payload directly to its Android targets. The malware, identified by researchers at NQ Mobile as "UpdtBot," disguises its malicious intentions by appearing as a text message telling recipients "their systems is at risk and they need to install the latest system upgrade." It is a typical scareware tactic, tricking would-be victims into believing they need to fix their phone or computer to stave off imminent harm. However, UpdtBot takes the traditional scam a step further. While most Android malware uses text messages to communicate with an attack server or to sign the victim up for text-message subscription services, this text-based threat contains a link in the message; when the user clicks on the link contained in the text, he/she is taken to a site that automatically uploads the malware. From there, UpdtBot can make calls, send texts, download new apps, and install corrupt software onto infected Android phones. So far, the malware infected more than 160,000 Android devices, according to NQ Mobile. Source: http://www.securitynewsdaily.com/1754-android-malware-text-messages.html

US-CERT: Social engineers target utilities with fake Microsoft support calls. The U.S. Cyber Emergency Response Team recently warned that cyber criminals are attempting highly targeted social engineering attacks on operators of industrial control systems. These utility companies are receiving phone calls warning of infected PCs. The utilities receive a call from a representative of a large software company — allegedly, the one that sold them the operating system on their computers — warning them their PCs have viruses and to take a series of steps so the caller can help the operator fix the problem. The calls purport to be from the "Microsoft Server Department" informing the utilities they have a virus. The caller tries to convince the utility operators to start certain services on their computer (likely, those services would allow unauthorized remote access). Source: http://www.networkworld.com/community/node/80337

5,000 malicious Android apps identified in Q1, 2012. Trend Micro released its quarterly report for the first part of 2012 and, so far, it appears cybercriminals focused their efforts mostly on schemes that target mobile device owners, particularly Android users. While 2011 was considered the year of the hacktivists, 2012 may be the year of mobile malware. At the end of 2011, many security experts said mobile threats would increase in 2012 and those predictions seem to be coming true. Trend Micro already identified 5,000 malicious Android apps, one-click billing fraud schemes, and fake applications that hide malicious elements being the most prevalent. Advanced persistent threats also left their mark on the first quarter. In these types of attacks, cybercriminals take their time to go deep into the targeted network and cause damage. Hoaxes and scams that circulate via e-mail and social networking sites were also prevalent. The large number of individuals that utilize Facebook, Twitter, and more recently, Pinterest, are all tempting targets for scammers and cybercrooks who use the data from social media sites to launch social engineering attacks. Source: http://news.softpedia.com/news/5-000-Malicious-Android-Apps-Identified-in-Q1-2012-265298.shtml

Gmail hit by massive outage: Up to 35 million affected. Google suffered a serious outage to its Gmail Web e-mail service April 17, which could have left up to 35 million users without access to their messages. The outage, which lasted for more than an hour, affected up to 10 percent of its global users, leaving them unable to access their personal e-mail accounts — and in some cases, their work e-mail. While many Gmail and Google Apps users in the United States were left without access, it appeared the United Kingdom, Europe, and Asia remained mostly unscathed. Google initially said the outage affected less than 2 percent of the Gmail user base, with the estimated 5.3 million affected users "unable to access Google Mail." Later, however, Google hiked the figure and said "less than 10 percent" of its user base was left without e-mail. Reports suggest that only the Web interface was affected by the outage, while those using IMAP/POP connections in a third-party desktop client, or mobile users, could still access their accounts and e-mail. Source: http://www.zdnet.com/blog/btl/gmail-hit-by-massive-outage-up-to-35-million-affected/74551

Google warns the operators of thousands of hacked web sites. The head of Google's Webspam team announced that Google sent out a message to the webmasters of 20,000 sites informing them their sites may have been hacked. In the e-mail message, the firm warned operators that the affected sites appear to be being used to redirect visitors to a malicious site.

Google asked the site administrators to check the files in their Web space for an eval(function(p,a,c,k,e,r) JavaScript code segment. The eval() function can be used to execute JavaScript character strings that may have previously been decrypted using an unpack feature. Google also warned of specially crafted .htaccess files. These may cause a file to be redirected only in certain circumstances, for example, when a visitor accesses the page via Google. Consequently, regular visitors to a site, such as the webmaster, will be unaware of the infection. The e-mail contains a link to Google's Webmaster Tools support page with instructions designed to help webmasters clean up their sites. Administrators were also being asked to close the security hole that was exploited to infect the site. Source: http://www.h-online.com/security/news/item/Google-warns-the-operators-of-thousands-of-hacked-web-sites-1542374.html

Malware disguised as new Instagram Android app. Instagram, the popular free photo sharing application for iOS devices, is now available for download for Android users on Google Play and Instagram's Web site. However, a rogue malicious version of the app is also being pushed to Russian Android users, offered from a Web page that mimics the legitimate one. Once the app is downloaded and run, it prompts users to send an SMS message to a premium rate number to "activate" the app, and then connects to specific sites, likely set to download other malware onto the users' device. Source: http://www.net-security.org/malware_news.php?id=2076&utm

Bogus 'Account limit exceeded' emails targeting Yahoo users. Fake Yahoo e-mail notifications are being sent to inboxes, urging users to verify their account because it "exceeded its limit," Hoax-Slayer warned. The message is accompanied by a veiled threat of account suspension within 24 hours aimed at making users panic, which raises the likelihood of them following the offered link. For users who follow the link, it leads to a fake Yahoo log-in page. Users who input their personal information send it to the phishers who created the page. This information is then used by the criminals to hijack the users' accounts. The accounts can be used for a variety of malicious schemes, including sending spam, bombarding the users' contacts with links leading to malware or making fake pleas for money. Source: http://www.net-security.org/secworld.php?id=12759&utm

Apple enhances Apple ID account security. iOS device owners whose Apple ID account may have triggered a flag with Apple's security team were asked to set up three new security questions and a backup e-mail address when they tried to download apps from the App Store. The request left some wondering whether they were subjected to a phishing attempt, as Apple did not announce or explain the move beforehand. However, the request was legitimate, as Apple confirmed for Ars Technica, and was part of the company's attempt to increase security. The measure was seen as a smart move by Apple, as the Apple ID account is tied to Apple's retail Web site and its media services. Many users have credit cards associated with their account. Source: http://www.net-security.org/secworld.php?id=12760&utm

Google hit with $25K fine, but FCC finds street view data collection not illegal. Google was issued a $25,000 fine by the Federal Communications Commission (FCC) for impeding the agency's investigation of some of the Internet search leader's data-gathering practices, PC

World reported April 15. At issue is the finding nearly 2 years ago that Google Street View cars were collecting payload data from unprotected Wi-Fi networks via code written for an experimental project. Now, the FCC, which is looking into what happened with the data and why it was gathered, ordered Google to open its checkbook because the company "deliberately impeded and delayed" its investigation, the New York Times reported. Google said it was "profoundly sorry for having mistakenly collected payload data — including personal information such as passwords and emails — from unencrypted networks." The FCC was initially satisfied with that response, but it said over time Google has repeatedly not responded to requests for information, took the position that searching employees' e-mails would be burdensome, and would not name the employees involved. Even so, the FCC decided Google's data collection was not illegal because the information the company gleaned was not encrypted. Source: http://www.cio.com/article/704305/Google_Hit_with_25K_Fine_but_FCC_Finds_Street_View_Data_Collection_Not_Illegal?taxonomyId=3234

Ransomware infects master boot record, Trend Micro finds. Researchers at Trend Micro uncovered a piece of ransomware targeting the master boot record (MBR) to take control of a system. The move is a step beyond typical pieces of ransomware, which usually encrypt files or restricts user access to the infected system. In this case, however, the malware copies the original MBR and overwrites it with its own malicious code. "Right after performing this routine, it automatically restarts the system for the infection to take effect," a threat response engineer at Trend Micro said. When the system restarts, the users are greeted with a message telling them their PC is now blocked and that they should pay 920 hryvnia (UAH) via the QIWI payment service to a purse number. Once that is done, the attacker promises to hand over a code to unlock the system, the researcher added. Source: http://www.securityweek.com/ransomware-infects-master-boot-record-trend-micro-finds

Researchers reveal flaws in Microsoft Partner Network Cloud Service. Experts from Vulnerability Lab have been helping Microsoft patch serious vulnerabilities that affected some services. The most important security hole was a persistent script code inject vulnerability found in Microsoft Partner Network Cloud service. To demonstrate their findings, the researchers made a video proof-of-concept that showed how easily an attacker can leverage the persistent script code injection flaws on a Microsoft Cloud aspx service to execute their own malicious code. Microsoft was notified regarding the presence of medium severity flaws in the Company & Mobile Phone Number (Profile) and the Company Name Profile Listing modules February 11. After collaborating with the Microsoft Security Response Center team and after ensuring the issues were addressed, Vulnerability Lab made available the video and a proof-of-concept in text format. Source: http://news.softpedia.com/news/Researchers-Reveal-Flaws-in-Microsoft-Partner-Network-Cloud-Service-264644.shtml

Malicious 'the Movie' apps served on Google Play. A number of 29 Android applications found on Google Play (the new Android Market) were identified as being malicious by Symantec. The pieces of malware, identified as Android.Dougalek, pretend to be popular games or games-related videos. First discovered in February, the elements were advertised as recipe apps, diet

assistant apps, content management apps, and adult apps. At the end of March, the same cybercriminals were believed to have launched another series of malicious programs, the names of which all end in "the Movie." Experts reveal that at least 70,000 users may have installed the pieces of software, but the true number of victims may be as high as 300,000. Initial analysis of the malevolent applications showed they mainly target Japanese Android users. Also, it is likely those who started the campaign are the same cybercriminals that spread the malware known as Android.Oneclickfraud. Once installed, the apps request the rights to access personal data and the phone's identity. While in the foreground it seems as they connect to an external server from which they download the promised videos, but in reality they gather information and send it back to the server. Once the malicious apps are installed, they will appear on the Android device under a different name than the one presented on Google Play. Currently, Google removed the applications from the Play site. Source: http://news.softpedia.com/news/Malicious-The-Movie-Apps-Served-on-Google-Play-264672.shtml

Two more Mac trojans discovered. Following the outbreak of the Flashback Mac trojan, security researchers spotted two more cases of Mac OS X malware. Both cases are variants on the same trojan, called SabPub, said a Kaspersky Lab researcher. The first variant is known as Backdoor.OSX.SabPub.a. Like Flashback, this new threat was likely spread through Java exploits on Web sites, and allows for remote control of affected systems. It was created roughly 1 month ago. However, the malware is not a threat to most users. It may have only been used in targeted attacks, the researcher said, with links to malicious Web sites sent via e-mail, and the domain used to fetch instructions for infected Macs has since been shut down. Furthermore, Apple's security update for Flashback helps render future Java-based attacks harmless. In addition to removing the Flashback malware, the update automatically deactivates the Java browser plug-in and Java Web Start if they remain unused for 35 days. Users must then manually re-enable Java when they encounter applets on a Web page or a Web Start application. Instead of attacking through malicious Web sites, the second SabPub variant uses infected Microsoft Word documents as vector, distributed by e-mail. Like the other SabPub variant, this one was used only in targeted attacks. Source: http://www.computerworld.com/s/article/9226234/Two_More_Mac_Trojans_Discovered

National Monuments and Icons

(Texas) **Officials: Fires overwhelmed resources.** Emergency officials could have tripled the manpower devoted to battling the late summer wildfires in 2011 in Bastrop, Texas, and it still would not been enough to stem the devastation, a legislative panel was told April 19. "There's not enough resources in Texas to prevent something like this happening," said the chief of emergency management for the Texas Department of Public Safety in testimony before the state house agriculture committee. Two people died from the fires that began swirling over the 2011 Labor Day weekend. More than 34,000 acres of pine forest and ranch land was scorched, an estimated 1,670 homes were destroyed, and 5,000-plus people were uprooted from their homes. More than 1,000 firefighters from across Texas and beyond the state's borders assisted in the effort to stop the flames. The Texas Air National Guard dumped 1.4 million gallons of

water on the flames, but it was of little use given the parched landscape and the buffeted winds. A major who commands the Texas National Guard, said the strained resources could be made worse the next time. He said the federal government is considering moving the state's fleet of eight C-130 heavy transport planes used in disasters to Montana. Source: http://www.kxan.com/dpp/news/local/bastrop/resources-were-no-match-for-bastrop-fire

Postal and Shipping

(Washington, D.C.) **Senate hit with 383 cases of dangerous, 'suspicious mail.** It has been over 10 years since the first anthrax mail attack against the U.S. Senate and authorities revealed that suspicious mail continues to flood in, so far with no injuries, the Washington Examiner reported April 18. The Senate Sergeant at Arms and Doorkeeper, revealed in budget testimony that the Senate Post Office intercepted 383 suspicious pieces of mail in 2011 "that were addressed to senators with the intent to disrupt Senate business." He reported all the suspect mail was reported to the U.S. Capitol Police. All incoming and internal mail is searched and scrubbed of contaminants before being delivered, he added. More than 300,000 items were tested in 2011. Source: http://washingtonexaminer.com/politics/washington-secrets/2012/04/senate-hit-383-cases-dangerous-suspicious-mail/504836

Bogus e-mails sent in postal scam. Some postal customers are receiving bogus e-mails about a package delivery or online postage charges, the Park Rapids Enterprise reported April 14. The e-mails contain a link or attachment that, when opened, installs a malicious virus that can steal personal information from computers. The e-mails claim to be from the U.S. Postal Service and contain fraudulent information about an attempted or intercepted package delivery or online postage charges. Like most viruses sent by e-mail, clicking on the link or opening the attachment will activate a virus that can steal information — such as user name, password, and financial account information. The U.S. Postal Inspection Service is working to resolve the issue and shut down the malicious program. Source: http://www.parkrapidsenterprise.com/event/article/id/32257/

Public Health

Wearable firewall stops pacemaker hacking. Security News Daily reported April 19 that researchers from Purdue and Princeton universities have developed a solution to what could be catastrophic problem for millions of people who use insulin pumps, pacemakers, and other personal medical devices that rely on wireless communication to function: MedMon — a signal-jamming personal firewall for medical devices that detects potentially malicious communications going into, or coming from, a wearable or implanted device. After identifying malicious signals, MedMon employs electronic jamming, similar to technology used in military systems, to prevent any potentially harmful wireless commands from getting through to the device and causing it to falter or accept instructions that could cause its wearer harm. The research team highlighted the need for its prototype by replicating, in the lab, an attack on a diabetes monitoring system, which consists of a continuous glucose monitor and an insulin pump that communicate wirelessly with each other. Analyzing a commercially available glucose

monitor, the scientists were able to eavesdrop on the wireless communication sent to the device — they used off-the-shelf software and hardware — and to reverse-engineer the communication protocol, discover the device PIN, and send their own malicious data to it, including instructions to start and stop insulin injection. Source: http://www.securitynewsdaily.com/1753-firewall-prevent-pacemaker-hacking.html

FDA safety communication: Bacteria found in Other-Sonic Generic Ultrasound Transmission Gel poses risk of infection. The U.S. Food and Drug Administration (FDA) received a report from a hospital that 16 patients had developed colonization or infection with the bacteria Pseudomonas aeruginosa, according to an April 18 FDA notice. Each patient was examined with transesophageal ultrasound probes using Other-Sonic Generic Ultrasound Transmission Gel. Upon investigation, the ugel was found to be contaminated with the bacteria Pseudomonas aeruginosa and Klebsiella oxytoca. Although Other-Sonic Generic Ultrasound Transmission Gel is not labeled as sterile or non-sterile, it is not sterile. At this time, the FDA is concerned about contamination of gel lot numbers 060111 through 120111. These lots contain both 250 milliliter bottles and 5 liter dispensing containers of gel. The lot number is printed on each bottle. The lots were manufactured June through December 2011 by Pharmaceutical Innovations. Not every patient exposed to Pseudomonas aeruginosa and Klebsiella oxytoca bacteria in Other-Sonic Generic Ultrasound Transmission Gel will develop colonization or infection, but the risk remains present. Source: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm299409.htm

Mobile tech, employee error blamed for rise in medical data breaches. Twenty-seven percent of the 250 U.S. health care providers included in a recent survey said they experienced at least one security breach in the past year, with employee error being the primary cause, Government Computer News reported April 16. The results of the "2012 HIMSS Analytics Report: Security of Patient Data," a biennial survey by Kroll Advisory Solutions, continued a trend in which health care data is increasingly being exposed. Past surveys found that 19 percent of respondents had experienced a breach in 2010, and 13 percent had in 2008. The survey report said 79 percent of the breaches were the result of employee actions, and that the mobility of patient data, resulting from new devices and technologies, was a major factor in patient data being exposed. Twenty-two percent of respondents said breaches resulted from mobile devices — laptop PCs, handheld devices, or portable hard drives — that were lost or stolen. More than 50 percent of the breaches were identified as "unauthorized access to information," most often a patient's name and birth date. Source: http://gcn.com/articles/2012/04/16/health-care-data-breaches-on-the-rise.aspx

Report: Nursing homes unprepared for natural disasters. Tornado, hurricane, or flood, nursing homes are woefully unprepared to protect frail residents in a natural disaster, government investigators say. The investigators from the inspector general's office of the Department of Health and Human Services noted that nearly 7 years after Hurricane Katrina's devastation of New Orleans exposed the vulnerability of nursing homes, shortcomings persist. "We identified many of the same gaps in nursing home preparedness and response," they wrote in the report released April 16. "Emergency plans lacked relevant information … Nursing homes faced

challenges with unreliable transportation contracts, lack of collaboration with local emergency management, and residents who developed health problems." Emergency plans required by the government often lack specific steps such as coordinating with local authorities, notifying relatives, or even pinning name tags and medication lists to residents during an evacuation, according to the findings. The report recommended that Medicare and Medicaid add specific emergency planning and training steps to the existing federal requirement that nursing homes have a disaster plan. Many such steps are in nonbinding federal guidelines that investigators found were disregarded. Source: http://www.washingtonpost.com/politics/report-nursing-homes-unprepared-for-natural-disasters/2012/04/15/gIQAhTP7KT_story.html

Transportation

(Florida) **Plane crash off Florida coast: Navy, Coast Guard search for pilot.** U.S. Coast Guard (USCG) and Navy forces were dispatched to the scene of a plane crash off the coast of Florida, the Los Angeles Times reported April 19. There was no word April 20 about the fate of the pilot believed to have become incapacitated at the controls. The small aircraft circled in the skies for hours over the Gulf of Mexico as air traffic controllers watched. They apparently tried for hours to make contact, but all attempts failed, pointing to the likelihood the pilot had perhaps fallen unconscious at the controls, or suffered a heart attack. The prospect of an unresponsive plane flying out of control sent up alarms: Two F-15 fighters under the direction of North American Aerospace Defense Command out of 159th Fighter Wing in New Orleans reached the aircraft. They also were unable to make contact with the pilot, said an April 19 statement. The USCG said the crash took place about 120 miles west of Tampa, in the gulf. The plane was completely submerged, no longer visible from the surface, officials said. Source: http://www.latimes.com/news/nation/nationnow/la-na-nn-florida-plane-crash-pilot-fate-unknown-20120419,0,5245736.story

Water and Dams

(Arizona) **Water vulnerability in U.S. border region.** A team of bilingual and binational researchers from the University of Arizona and the Colegio de Sonora in Hermosillo, Sonora, Mexico, issued a casebook that depicts the water vulnerability and potential adaptation to climate change throughout the Arizona-Sonora region, a University of Arizona release reported April 16. For the last 3 years, the research team has worked closely with water managers, disaster relief planners, and other decision-makers in Arizona and Sonora to assess the capacity that governments, private enterprises, and individuals might have to better prepare for, or adapt to, such changes. Researchers found increased vulnerability of urban water users to climatic changes because of factors such as aging or inadequate water-delivery infrastructure, over-allocation of water resources within the region, and the location of poor neighborhoods in flood-prone areas or other areas at risk. Adding to vulnerability issues, agriculture was noted as consuming approximately 70 to 80 percent of available water in the Arizona-Sonora region. Source: http://www.homelandsecuritynewswire.com/dr20120418-water-vulnerability-in-u-s-border-region

DEP: Chemical in New Hanover wells unexpected from petroleum spill. State officials were unsure how a complicated mixture of dangerous organic chemicals made its way into five New Hanover, Pennsylvania residential wells along Route 663. Officials from the Pennsylvania Department of Environmental Protection told residents and officials April 17 they are focusing on the site of the former Good Oil Co. where dozens of tanks ranging in size and contents have been located for years. Contaminants associated with petroleum products — such as benzene and MTBE — were found in wells as well as more peculiar "volatile organic compounds." The chemicals are not normally associated with petroleum businesses. It is too soon, officials said, to say how the matter will be resolved, however, the usual solutions include bottle water, carbon filters, reverse osmosis filters, and connection to public water. Source: http://www.pottsmerc.com/apps/pbcs.dll/article?AID=/20120418/NEWS01/120419405/dep-chemical-in-new-hanover-wells-unexpected-from-petroleum-spill-(video) http://www.pottsmerc.com/apps/pbcs.dll/article?AID=/20120418/NEWS01/120419405/dep-chemical-in-new-hano-###

Army Corps getting ready for 'big water' in northwest. Federal water and dam managers in the pacific northwest are draining reservoirs in the Columbia and Snake River basins to get ready for "big water" coursing downriver, Northwest News Network reported April 16. The U.S. Army Corps of Engineers called for bigger drawdowns, or drafting, to protect against flooding. A supervisory engineer said more room is needed to catch runoff from the bountiful snows of March. "Grand Coulee is being drafted close to 2 feet per day, which is quite a bit ... Dworshak (Dam) is also drafting fairly steeply..." The engineer said water is being spilled over the tops of many federal dams to speed young salmon on their way to the ocean. He said river managers will move aggressively to refill reservoirs later this spring after the flood danger has passed. The steep drawdown of the Grand Coulee reservoir (Lake Roosevelt) may force a temporary suspension of service on the Inchelium-Gifford ferry in late April. Source: http://news.opb.org/article/army_corps_getting_ready_for_big_water_in_northwest/

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168